



**GUIDELINES FOR THE
INTERNAL AUDIT FUNCTION IN BANKS**

Date: 2 January 2018

CONTENTS

PRINCIPLES :	3
I. SUPERVISORY EXPECTATIONS RELEVANT TO THE INTERNAL AUDIT FUNCTION	5
A. INDEPENDENCE AND OBJECTIVITY	5
B. PROFESSIONAL COMPETENCE, DUE PROFESSIONAL CARE AND PROFESSIONAL ETHICS	7
II. SCOPE OF ACTIVITIES	10
A. INCLUSION OF ALL ACTIVITIES	10
B. MATTERS OF REGULATORY INTEREST	11
III. CORPORATE GOVERNANCE MATTERS	14
A. PERMANENCY OF INTERNAL AUDIT FUNCTION	14
B. RESPONSIBILITY OF THE BOARD OF DIRECTORS AND SENIOR MANAGEMENT	15
C. RESPONSIBILITIES OF THE AUDIT COMMITTEE IN RELATION TO INTERNAL AUDIT	16
D. MANAGEMENT OF THE INTERNAL AUDIT DEPARTMENT	17
E. REPORTING LINES OF THE INTERNAL AUDIT FUNCTION	18
F. RELATIONSHIP BETWEEN INTERNAL AUDIT, COMPLIANCE & RISK MANAGEMENT FUNCTIONS	19
G. INTERNAL AUDIT WITHIN A GROUP OR HOLDING COMPANY STRUCTURE	20
H. OUTSOURCING OF INTERNAL AUDIT ACTIVITIES	21
IV. RELATIONSHIP BETWEEN AMBD AND THE INTERNAL AUDIT FUNCTION	22
A. COMMUNICATION	22
B. SUPERVISORY ASSESSMENT OF INTERNAL AUDIT FUNCTION	25
C. EARLY REMEDIAL ACTION BY AMBD	27
V. RESPONSIBILITIES OF A BANK’S AUDIT COMMITTEE	30
Financial reporting, including disclosures	30
Internal control	30
Audit	31
The statutory audit or external audit.....	31
Remedial actions	32

PRINCIPLES :

- Principle 1 : An effective internal audit function's prime purpose is to provide independent assurance to the board of directors and senior management on the quality and effectiveness of a bank's internal control, risk management and governance systems and processes, thereby helping the board and senior management protect their organisation and its reputation.
- Principle 2 : The bank's internal audit function must be independent of the audited activities, which requires the internal audit function to have sufficient standing and authority within the bank, thereby enabling internal auditors to carry out their assignments with objectivity.
- Principle 3 : Professional competence, including the knowledge and experience of each internal auditor and of internal auditors collectively, is essential to the effectiveness of the bank's internal audit function.
- Principle 4 : Internal auditors must act with integrity.
- Principle 5 : Each bank must have an internal audit charter that articulates the purpose, standing and authority of the internal audit function within the bank in a manner that promotes an effective internal audit function as described in Principle 1.
- Principle 6 : Every activity (including outsourced activities) and every entity of the bank must fall within the overall scope of the internal audit function.
- Principle 7 : The scope of the internal audit function's activities must ensure adequate coverage of matters of regulatory interest within the audit plan.
- Principle 8 : Each bank must have a permanent internal audit function, which must be structured consistent with Principle 14 when the bank is within a banking group or holding company.
- Principle 9 : The bank's board of directors has the ultimate responsibility for ensuring that senior management establishes and maintains an adequate, effective and efficient internal control system and, accordingly, the board must support the internal audit function in discharging its duties effectively.
- Principle 10 : The audit committee must oversee the bank's internal audit function.
- Principle 11 : The head of the internal audit department must be responsible for ensuring that the department complies with sound internal auditing standards and with a relevant code of ethics.

- Principle 12 : The internal audit function must be accountable to the audit committee on all matters related to the performance of its mandate as described in the internal audit charter.
- Principle 13 : The internal audit function must independently assess the effectiveness and efficiency of the internal control, risk management and governance systems and processes created by the business units and support functions and provide assurance on these systems and processes.
- Principle 14 : To facilitate a consistent approach to internal audit across all the banks within a banking organisation, the board of directors of each bank within a banking group or holding company structure must ensure that either
- (i) the bank has its own internal audit function which must be accountable to the bank's board and must report to the banking group or holding company's head of internal audit; or
 - (ii) the banking group or holding company's internal audit function performs internal audit activities of sufficient scope at the bank to enable the board to satisfy its fiduciary and legal responsibilities.
- Principle 15 : If a bank chooses to outsource certain aspects of internal audit, the board of directors remains ultimately responsible for the internal audit function.
- Principle 16 : The AMBD and the bank's internal auditors will conduct at least one meeting per year to: (i) discuss the risk areas identified by both parties; (ii) understand the risk mitigation measures taken by the bank; and (iii) monitor the bank's response to weaknesses identified.
- Principle 17 : The AMBD will assess annually whether the internal audit function has sufficient standing and authority within the bank and operates according to sound principles.
- Principle 18 : The AMBD will formally report all weaknesses they identify in the internal audit function to the board of directors and require timely remedial actions. The AMBD will take informal or formal supervisory actions requiring the board and senior management to remedy any identified deficiencies related to the internal audit function within a specified timeframe and to provide periodic written progress reports.
- Principle 19 : The AMBD will consider the impact of its assessment of the internal audit function on its evaluation of the bank's risk profile and on its own supervisory work.
- Principle 20 : The AMBD will take informal or formal supervisory actions requiring the board and senior management to remedy any identified deficiencies related to the internal audit function within a specified timeframe and to provide the supervisor with periodic written progress reports.

I. SUPERVISORY EXPECTATIONS RELEVANT TO THE INTERNAL AUDIT FUNCTION

A. INDEPENDENCE AND OBJECTIVITY

Principle :

1. An effective internal audit function's prime purpose is to provide independent assurance to the board of directors and senior management on the quality and effectiveness of a bank's internal control, risk management and governance systems and processes, thereby helping the board and senior management protect their organisation and its reputation.

Guidelines:

- 1.1 The internal audit function plays a crucial role in the ongoing maintenance and assessment of a bank's internal control, risk management and governance systems and processes – areas in which the AMBD has a keen interest. Furthermore, both internal auditors and the AMBD use risk based approaches to determine their respective work plans and actions. While internal auditors and the AMBD each have a different mandate and are responsible for their own judgments and assessments, they may identify the same or similar/related risks.
- 1.2 The internal audit function must develop an independent and informed view of the risks faced by the bank based on their access to all bank records and data, their enquiries, and their professional competence. The internal audit function must be able to discuss their views, findings and conclusions directly with the audit committee, thereby helping the board to oversee senior management.
- 1.3 A branch of a foreign bank licensed as a bank in Brunei Darussalam (Brunei branch of a foreign bank) must provide the AMBD with a satisfactory explanation how the bank's board of directors and senior management formalize and discharge their respective oversight responsibilities in relation to the Brunei branch of the foreign bank. This includes their responsibilities in terms of these Guidelines.

Principle:

2. The bank's internal audit function must be independent of the audited activities, which requires the internal audit function to have sufficient standing and authority within the bank, thereby enabling internal auditors to carry out their assignments with objectivity.

Guidelines:

- 2.1 On the basis of the audit plan established by the head of the internal audit function and approved by the board of directors, the internal audit function must be able to perform its assignments on its own initiative in all areas and functions of the bank. It must be free to report its findings and assessments internally through clear reporting lines. The head of internal audit must demonstrate appropriate leadership and have the necessary skills to fulfil his or her responsibility for maintaining the function's independence and objectivity.
- 2.2 The internal audit function must not be involved in designing, selecting, implementing or operating specific internal control measures. However, the independence of the internal audit function must not prevent senior management from requesting input from internal audit on matters related to risk and internal controls which would not impair the independence, objectivity and effectiveness of the internal audit function. Nevertheless, the development and implementation of internal controls must remain the responsibility of management.
- 2.3 Continuously performing similar tasks or routine jobs may negatively affect an individual internal auditor's capacity for critical judgement because of possible loss of objectivity. It is therefore a sound practice, whenever practicable and without jeopardising competence and expertise, to periodically rotate internal audit staff within the internal audit function. In addition, a bank may rotate staff from other functional areas of the bank to the internal audit function or from the internal audit function to other functional areas of the bank. Staff rotations within the internal audit function and staff rotations to and from the internal audit function must be governed by and conducted in accordance with a sound written policy. The policy must be designed to avoid conflicts of interest, including the observance of an appropriate "cooling-off" period following an individual's return to the internal audit staff before that individual audits activities in the functional area of the bank where his/her rotation had been served.
- 2.4 The independence and objectivity of the internal audit function may be undermined if the internal audit staff's remuneration is linked to the financial performance of the business lines for which they exercise internal audit responsibilities. The remuneration of the head of the internal audit function must be determined in accordance with the remuneration policies and practices of the bank. Remuneration to reward the performance of the head of internal audit or internal audit staff members must be structured to avoid creating conflicts of interest and compromising independence and objectivity.

B. PROFESSIONAL COMPETENCE, DUE PROFESSIONAL CARE AND PROFESSIONAL ETHICS

Principle:

3. Professional competence, including the knowledge and experience of each internal auditor and of internal auditors collectively, is essential to the effectiveness of the bank's internal audit function.

Guidelines:

- 3.1 Professional competence depends on the auditor's capacity to collect and understand information, to examine and evaluate audit evidence and to communicate with the stakeholders of the internal audit function. This must be combined with suitable comprehensive methodologies and tools and sufficient knowledge of auditing techniques.
- 3.2 The head of internal audit must be responsible for acquiring human resources with sufficient qualifications and skills to effectively deliver on the mandate for professional competence and to audit to the required level. He/she must continually assess and monitor the skills necessary to do so. The skills required for senior internal auditors must include the abilities to judge outcomes and make an impact at the highest level of the organisation.
- 3.3 The head of internal audit must ensure that the internal audit staff acquires appropriate ongoing training in order to meet the growing technical complexity of banks' activities and the increasing diversity of tasks that need to be undertaken as a result of the introduction of new products and processes within banks and other developments in the financial sector.
- 3.4 Internal auditors collectively must be competent to examine all areas in which the bank operates. Alternatively, when outsourcing arrangements are in place, it is the responsibility of the head of internal audit to maintain adequate oversight and to ensure adequate transfer of knowledge from external experts to the bank's internal audit staff. The head of internal audit must ensure that the use of those experts does not compromise the independence and objectivity of the internal audit function.
- 3.5 Internal auditors must apply the care and skills expected of a reasonably prudent and competent professional. Due professional care does not imply infallibility; however, internal auditors with limited competence or experience in particular areas must be supervised by experienced internal auditors.

Principle:

4. Internal auditors must act with integrity.

Guidelines:

- 4.1 Integrity establishes trust as it requires the internal auditor to be straightforward, honest and truthful. This provides the basis for reliance on the internal auditor's professional judgement.
- 4.2 Internal auditors must respect the confidentiality of information acquired in the course of their duties. They must not use that information for personal gain or malicious action and must be diligent in the protection of information acquired.
- 4.3 The head of the internal audit function and all internal auditors must avoid conflicts of interest. Internally recruited internal auditors must not engage in auditing activities for which they have had previous responsibility before a sufficiently long "cooling off" period has elapsed. Moreover, compensation arrangements must not provide incentives for internal auditors to act contrary to the attributes and objectives of the internal audit function.
- 4.4 Internal auditors must apply the bank's code of ethics (when there is one) or must adhere to an established international code of ethics for internal auditors, such as that of The Institute of Internal Auditors. A code of ethics must at a minimum address the principles of objectivity, competence, confidentiality and integrity.

Principle:

5. Each bank must have an internal audit charter that articulates the purpose, standing and authority of the internal audit function within the bank in a manner that promotes an effective internal audit function as described in Principle 1.

Guidelines:

- 5.1 The charter must be drawn up and reviewed periodically by the head of internal audit and approved by the board of directors. It must be available to all internal stakeholders of the organisation and, in certain circumstances, such as listed banks, to external stakeholders.
- 5.2 At a minimum, an internal audit charter must establish:
- (a) The internal audit function's standing within the bank, its authority, its responsibilities and its relations with other control functions in a manner that promotes the effectiveness of the function as described in Principle 1 of this paper;
 - (b) The purpose and scope of the internal audit function;
 - (c) The key features of the internal audit function described under Principles 2, 3 and 4 above;
 - (d) The obligation of the internal auditors to communicate the results of their engagements and a description of how and to whom this must be done (reporting line);
 - (e) The criteria for when and how the internal audit function may outsource some of its engagements to external experts;
 - (f) The terms and conditions according to which the internal audit function can be called upon to provide consulting or advisory services or to carry out other special tasks;
 - (g) The responsibility and accountability of the head of internal audit;
 - (h) A requirement to comply with sound internal auditing standards;
 - (i) Procedures for the coordination of the internal audit function with the statutory or external auditor.
- 5.3 The charter must empower the internal audit function, whenever relevant to the performance of its assignments, to initiate direct communication with any member of staff, to examine any activity or entity of the bank, and to have full and unconditional access to any records, files, data and physical properties of the bank. This includes access to management information systems and records and the minutes of all consultative and decision-making bodies.

II. SCOPE OF ACTIVITIES

A. INCLUSION OF ALL ACTIVITIES

Principle:

6. Every activity (including outsourced activities) and every subsidiary of the bank must fall within the overall scope of the internal audit function.

Guidelines:

- 6.1 The scope of internal audit activities must include the examination and evaluation of the effectiveness of the internal control, risk management and governance systems and processes of the entire bank, including its outsourced activities, and its subsidiaries and branches.
- 6.2 The internal audit function must independently evaluate the:
- (a) Effectiveness and efficiency of internal control, risk management and governance systems in the context of both current and potential future risks;
 - (b) Reliability, effectiveness and integrity of management information systems and processes (including relevance, accuracy, completeness, availability, confidentiality and comprehensiveness of data);
 - (c) Monitoring of compliance with laws and regulations, including any requirements from the AMBD and other supervisory bodies (see the following sub-section for more details); and
 - (d) Safeguarding of assets.
- 6.3 The head of internal audit is responsible for establishing an annual internal audit plan that can be part of a multi-year plan. The plan must be based on a robust risk assessment (including input from senior management and the board) and must be updated at least annually (or more frequently to enable an ongoing real-time assessment of where significant risks lie). The board's approval of the audit plan requires that an appropriate budget will be available to support the internal audit function's activities. The budget must be sufficiently flexible to adapt to variations in the internal audit plan in response to changes in the bank's risk profile.

B. MATTERS OF REGULATORY INTEREST

Principle:

7. The scope of the internal audit function's activities must ensure adequate coverage of matters of regulatory interest within the audit plan.

Guidelines:

- 7.1 Internal audit must have the appropriate capability regarding matters of regulatory interest and undertake regular reviews of such areas based on the results of its robust risk assessment. These include policies, processes and governance measures established in response to various regulatory principles, rules and guidance established by the AMBD with special regard to the Guidelines of Corporate Governance (for banks). In particular, the internal audit function of a bank must have the capacity to review key risk functions such as :-
- i. Risk Management;
 - ii. Capital adequacy and liquidity control functions;
 - iii. Regulatory and internal reporting functions;
 - iv. The regulatory compliance function;
 - v. The finance function; and

Risk management

- 7.2 A bank's risk management processes support and reflect its adherence to regulatory requirements and safe and sound banking practices. Therefore, internal audit must include in its scope the following aspects of risk management:
- (a) the organisation and mandates of the risk management function including market, credit, liquidity, interest rate, operational, and legal risks;
 - (b) evaluation of risk appetite, escalation and reporting of issues and decisions taken by the risk management function;
 - (c) the adequacy of risk management systems and processes for identifying, measuring, assessing, controlling, responding to, and reporting on all the risks resulting from the bank's activities;
 - (d) the integrity of the risk management information systems, including the accuracy, reliability and completeness of the data used; and

- (e) the approval and maintenance of risk models including verification of the consistency, timeliness, independence and reliability of data sources used in such models.

When the risk management function has not informed the board of directors about the existence of a significant divergence of views between senior management and the risk management function regarding the level of risk faced by the bank, the head of internal audit must inform the board about this divergence.

Capital adequacy and liquidity

- 7.3 Banks are subject to the AMBD's regulatory framework for capital adequacy and liquidity. The scope of internal audit must include all provisions of this regulatory framework and in particular the bank's system for identifying and measuring its regulatory capital and assessing the adequacy of its capital resources in relation to the bank's risk exposures and required minimum capital ratios.
- 7.4 Internal audit must review management's process for stress testing capital levels, taking into account the frequency of such exercises, their purpose (e.g., internal tests vs. AMBD tests), the reasonableness of scenarios and the underlying assumptions employed, and the reliability of the processes used.
- 7.5 Additionally, the bank's systems and processes for measuring and monitoring its liquidity positions in relation to its risk profile, external environment, and minimum regulatory requirements, must fall within the audit universe.

Regulatory and internal reporting

- 7.6 In addition to the matters identified above, internal auditors must regularly evaluate the effectiveness of the process by which the risk and reporting functions interact to produce timely, accurate, reliable and relevant reports for both internal management and the AMBD. This includes standardised reports which record the bank's calculation of its capital resources, requirements and ratios. It may also include public disclosures intended to facilitate transparency and market discipline such as Basel II Pillar 3 disclosures and the reporting of regulatory matters in the bank's public reports.

Compliance

- 7.7 Internal audit must review the scope of the activities of the compliance function periodically.
- 7.8 Compliance must cover laws, rules and standards, including primary legislation, rules and standards issued by legislators and supervisors, market conventions, codes of practice promoted by industry associations, and internal codes of conduct applicable to the staff members of the bank.
- 7.9 The audit of the compliance function must include an assessment of how effectively the compliance function fulfils its responsibilities.

Finance

- 7.10 A bank's finance function is responsible for the integrity and accuracy of financial data and reporting. Key aspects of Finance's activities (e.g. calculations, profit and loss valuations and reserves) have an impact on the level of a bank's capital resources and therefore associated controls must be robust and consistently applied across business lines. It is important that these controls are subject to periodic internal audit review, using expertise to provide an effective evaluation of bank practices.
- 7.11 Internal audit must devote sufficient resources to evaluate the valuation control environment, availability and reliability of information or evidence used in the valuation process and the reliability of estimated fair values. This is achieved through reviewing the independent price verification processes and testing valuations of significant transactions.
- 7.12 Internal audit must also include in its scope (the list is not intended to be exhaustive):
- (a) The organisation and mandate of the finance function;
 - (b) The adequacy and integrity of underlying financial data and finance systems and processes for completely identifying, capturing, measuring and reporting key data such as profit or loss, valuations of financial instruments and impairment allowances;
 - (c) The approval and maintenance of pricing models including verification of the consistency, timeliness, independence and reliability of data sources used in such models;
 - (d) Controls in place to prevent and detect trading irregularities;
 - (e) Balance sheet controls including key reconciliations performed and actions taken (e.g. adjustments).

III. CORPORATE GOVERNANCE MATTERS

A. PERMANENCY OF INTERNAL AUDIT FUNCTION

Principle:

8. Each bank must have a permanent internal audit function, which must be structured consistent with Principle 14 when the bank is within a banking group or holding company.

Guidelines:

- 8.1 In fulfilling its duties and responsibilities, senior management and the board must take all the necessary measures to ensure that the bank has a permanent internal audit function commensurate with its size, the nature of its operations and the complexity of its organisation.
- 8.2 Internal audit activities must normally be conducted by the bank's own internal audit staff. If certain internal audit activities are outsourced, the board of directors remains ultimately responsible for these activities and for maintaining an internal audit function within the bank (see Principle 15).

B. RESPONSIBILITY OF THE BOARD OF DIRECTORS AND SENIOR MANAGEMENT

Principle:

9. The bank's board of directors has the ultimate responsibility for ensuring that senior management establishes and maintains an adequate, effective and efficient internal control system and, accordingly, the board must support the internal audit function in discharging its duties effectively.

Guidelines:

- 9.1 At least once a year, the board of directors must review the effectiveness and efficiency of the internal control system based, in part, on information provided by the internal audit function. Moreover, as part of their oversight responsibilities, the board of directors must review the performance of the internal audit function. From time to time, the board of directors must consider commissioning an independent external quality assurance review of the internal audit function.
- 9.2 Senior management is responsible for developing an internal control framework that identifies, measures, monitors and controls all risks faced by the bank. It must maintain an organisational structure that clearly assigns responsibility, authority and reporting relationships and ensures that delegated responsibilities are effectively carried out. Senior management must report to the board of directors on the scope and performance of the internal control framework.
- 9.3 Senior management must inform the internal audit function of new developments, initiatives, projects, products and operational changes and ensure that all associated risks, known and anticipated, are identified and communicated at an early stage.
- 9.4 Senior management must be accountable for ensuring that timely and appropriate actions are taken on all internal audit findings and recommendations.
- 9.5 Senior management must ensure that the head of internal audit has the necessary resources, financial and otherwise, available to carry out his or her duties commensurate with the annual internal audit plan, scope and budget approved by the audit committee.

C. RESPONSIBILITIES OF THE AUDIT COMMITTEE IN RELATION TO INTERNAL AUDIT

Principle:

10. The audit committee must oversee the bank's internal audit function.

Guidelines:

- 10.1 The oversight function of the audit committee includes ensuring that the internal audit function is able to discharge its responsibilities in an independent manner, congruent with principle 2. It also includes reviewing and approving the audit plan, its scope, and the budget of the internal audit function. It reviews key audit reports and ensures that senior management is taking necessary and timely corrective actions to address control weaknesses, compliance issues with policies, laws and regulations and other concerns identified and reported by the internal audit function.
- 10.2 Section V of this document gives a more detailed list of the responsibilities of an audit committee.

D. MANAGEMENT OF THE INTERNAL AUDIT DEPARTMENT

Principle:

11. The head of the internal audit department must be responsible for ensuring that the department complies with sound internal auditing standards and with a relevant code of ethics.

Guidelines:

- 11.1 The head of the internal audit department must ensure compliance with sound internal auditing standards, such as The Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing. In addition, auditors must adhere to a relevant code of ethics (see Principle 4).
- 11.2 The audit committee must ensure that the head of the internal audit function is a person of integrity. This means that he or she will be able to perform his or her work with honesty, diligence and responsibility. It also implies that this person observes the law and has not been a party to any illegal activity. The head of internal audit must also ensure that the members of internal audit staff are persons of integrity.

E. REPORTING LINES OF THE INTERNAL AUDIT FUNCTION

Principle:

12. The internal audit function must be accountable to the board, or its audit committee, on all matters related to the performance of its mandate as described in the internal audit charter.

Guidelines:

- 12.1 The Internal audit function must be accountable to the board of directors or its audit committee. It must also promptly inform senior management about its findings.

- 12.2 Senior management is responsible for implementing and maintaining an adequate and effective internal control system and processes. Therefore, the internal audit function must inform senior management of all significant findings so that timely corrective actions can be taken. Subsequently, the internal audit function must follow up with senior management on the outcome of these corrective measures. The head of the internal audit function must report to the board, or its audit committee, the status of findings that have not (yet) been rectified by senior management.

F. RELATIONSHIP BETWEEN INTERNAL AUDIT, COMPLIANCE & RISK MANAGEMENT FUNCTIONS

Principle:

13. The internal audit function must independently assess the effectiveness and efficiency of the internal control, risk management and governance systems and processes created by the business units and support functions and provide assurance on these systems and processes.

Guidelines:

13.1 The relationship between a bank's business units, the support functions and the internal audit function can be explained using the three lines of defence model.

13.1.1 The business units are the first line of defence. They undertake risks within assigned limits of risk exposure and are responsible and accountable for identifying, assessing and controlling the risks of their business.

13.1.2 The second line of defence includes the support functions, such as risk management, compliance, legal, human resources, finance, operations, and technology. Each of these functions, in close relationship with the business units, ensures that risks in the business units have been appropriately identified and managed. The business support functions work closely to help define strategy, implement bank policies and procedures, and collect information to create a bank-wide view of risks.

13.1.3 The third line of defence is the internal audit function that independently assesses the effectiveness of the processes created in the first and second lines of defence and provides assurance on these processes.

Line of defence	Examples	Approach
First line	Front Office, any client-facing activity	Transaction-based, ongoing
Second line	Risk Management, Compliance, Legal, Human Resources, Finance, Operations, and Technology	Risk-based, ongoing or periodic
Third line	Internal Audit	Risk-based, periodic

13.2 The responsibility for internal control does not transfer from one line of defence to the next line.

G. INTERNAL AUDIT WITHIN A GROUP OR HOLDING COMPANY STRUCTURE

Principle:

14. To facilitate a consistent approach to internal audit across all the banks within a banking organisation, the board of directors of each bank within a banking group or holding company structure must ensure that either:
- i. the bank has its own internal audit function which must be accountable to the bank's board and must report to the banking group or holding company's head of internal audit; or
 - ii. the banking group or holding company's internal audit function performs internal audit activities of sufficient scope at the bank to enable the board to satisfy its fiduciary and legal responsibilities.

Guidelines:

- 14.1 The board of directors of each bank in a group or holding company structure remains responsible for ensuring that the bank's senior management establishes and maintains an adequate, effective and efficient internal control system and processes. The board also must ensure that internal audit activities are conducted effectively at the bank according to the principles of this document. The internal auditors who perform the internal audit work at the bank must report to the bank's audit committee and to the group or holding company's head of internal audit.
- 14.2 The board of directors and senior management of the parent company have the overall responsibility for ensuring that an adequate and effective internal audit function is established across the banking organisation and for ensuring that internal audit policies and mechanisms are appropriate to the structure, business activities and risks of all the components of the group.
- 14.3 The head of internal audit at the level of the parent company must define the group internal audit strategy, determine the organisation of the internal audit function both at the parent and subsidiary bank levels (in consultation with these entities' respective boards of directors and in accordance with local laws) and formulate the internal audit principles, which include the audit methodology and quality assurance measures.
- 14.4 The group internal audit function must determine the audit scope for the banking organisation. In doing so, it must comply with local legal and regulatory provisions and incorporate local knowledge and experience.

H. OUTSOURCING OF INTERNAL AUDIT ACTIVITIES

Principle:

15. If a bank chooses to outsource certain aspects of internal audit, the board of directors remains ultimately responsible for the internal audit function.

Guidelines:

- 15.1 Banks must have permanent internal audit functions using their own staff. However, outsourcing of internal audit activities, but not the function, on a limited and targeted basis can bring benefits to banks such as access to specialised expertise and knowledge for an internal audit engagement where the expertise is not available within the internal audit function. Outsourcing could also alleviate temporary resourcing constraints which might otherwise jeopardise the execution of the audit plan. Banks must seek prior approval from the AMBD for outsourcing specific internal audit activities.
- 15.2 The head of internal audit must ensure that any outsourcing supplier complies with the principles of the bank's internal audit charter. To preserve independence, it is important to ensure that
- 15.2.1 the supplier has not been previously engaged in a consulting engagement in the same area within the bank unless a reasonably long "cooling-off" period has elapsed.
- 15.2.2 experts who participate in an internal audit engagement are not allowed to provide consulting services to a function of the bank they have audited within the last five years. Additionally, banks are not allowed to outsource internal audit activities to their own external audit firm.
- 15.3 The head of internal audit must ensure that, whenever practical, the relevant knowledge input from an expert is assimilated into the organisation. This may be possible by having one or more members of the bank's internal audit staff participate in the external expert's work.
- 15.4 Any outsourcing activities done by the bank must be read together with the Outsourcing Guidelines issued by AMBD.

IV. RELATIONSHIP BETWEEN AMBD AND THE INTERNAL AUDIT FUNCTION

A. COMMUNICATION

Principle:

16. The AMBD and the bank's internal auditors will conduct at least one meeting per year to: (i) discuss the risk areas identified by both parties; (ii) understand the risk mitigation measures taken by the bank; and (iii) monitor the bank's response to weaknesses identified.

Guidelines:

- 16.1 The internal audit function is a key building block of the internal control system because it provides an independent assessment of the adequacy of, and compliance with, the bank's established policies and procedures. Therefore, the AMBD has an interest in engaging in a constructive and formalised dialogue with the internal audit function on the quality of the internal control system.
- 16.2 The extent to which the work of internal auditors is factored into the supervisory course of action for a bank will depend on the AMBD's supervisory approach, the AMBD's assessment of the internal audit function, and the circumstances relating to the issues at hand.
- 16.3 In addition to meetings with senior management, the AMBD will conduct an annual or more frequent meeting with the bank's internal auditors to discuss their risk analysis, findings, recommendations and the audit plan. The AMBD reserves the right to decide whether senior management must or must not be present at these meetings. These meetings can also facilitate the understanding of how and to what extent the recommendations made by the AMBD (including those made during on-site reviews) and internal auditors have been implemented. The AMBD may also request the internal audit reports from time to time.
- 16.4 The relationship between the AMBD and internal auditors is also two-way. The AMBD may share relevant information with the internal audit function when this increases the effectiveness of its internal audit work. These meetings will be sufficiently frequent to enable the AMBD to ensure the effectiveness of the actions taken by the bank to carry out these recommendations. The frequency of these meetings and other communication between supervisors and internal auditors will be commensurate with the bank's size, the nature and risks of its operations and the complexity of its organization. The AMBD will request the internal audit reports from time to time. The analysis of these internal audit reports and information may contribute to the AMBD's assessment of the internal control systems of the bank. The AMBD may make specific recommendations for strengthening the internal audit function and the control environment.

- 16.5 A bank's capital and liquidity positions and its processes and methods for determining, monitoring, controlling and reporting on material risks are directly relevant and important to the AMBD. Therefore, the AMBD and internal auditors must discuss the areas described in Principle 7.
- 16.6 Internal audit is well placed to provide the AMBD with insight on the bank's business model including risks in the bank's business activities, processes and functions and the adequacy of the control and oversight of these risks such as:
- (a) Application and effectiveness of risk management procedures and risk assessment methodologies, as applied to credit risk, market risk, liquidity risk, operational risk (including information technology and business continuity management), and other risks relevant to the Basel II Pillar 2 requirements;
 - (b) Contingency planning;
 - (c) Outsourcing arrangements; and
 - (d) Fraud risk.
- 16.7 To the extent that accounting data drives certain regulatory measures or is included in regulatory reporting, such meetings must include discussion of work performed by internal audit relating to:
- (a) Measurement (including fair values) and impairment of financial instruments;
 - (b) Significant transactions in financial instruments with a regulatory impact; and
 - (c) Other judgemental accounting areas, including estimates.
- 16.8 The meetings must also cover business or market conduct issues as identified through the audit of the compliance function, for example:
- (a) Transaction reporting;
 - (b) Adherence to rules for dealing with client assets;
 - (c) Anti-money laundering processes and controls; and
 - (d) Management of conflicts of interest.

- 16.9 The board of directors and senior management are responsible for establishing the bank's strategy and business models. However, changes therein may have consequences for the bank's internal control, risk management and governance systems and processes. Although internal audit does not set the bank's policies and must not interfere in its business decisions, it can be in a position to influence them by challenging management. Both the internal audit function and the AMBD have an interest in the following:
- (a) Processes for objective setting and strategic decision making; and
 - (b) Quality and substance of management and governance structure and processes.

B. SUPERVISORY ASSESSMENT OF INTERNAL AUDIT FUNCTION

Principle:

17. The AMBD will assess annually whether the internal audit function has sufficient standing and authority within the bank and operates according to sound principles.

Guidelines:

- 17.1 The AMBD will consider the extent to which the board of directors, its audit committee and senior management promote a strong internal control environment supported and assessed by a sound internal audit function. This assessment will influence the overall assessment of the bank and enable the AMBD to determine the extent to which the AMBD will use the work of the internal audit function.
- 17.2 The assessment of the internal audit function must be based on the supervisory expectations as set out in section I of this paper. This includes:
- (a) The basic features of the internal audit function;
 - (b) The internal audit function's standing and authority within the bank;
 - (c) The existence and content of the internal audit charter;
 - (d) The scope of the internal audit function's work and its output;
 - (e) The corporate governance arrangements that apply to the internal audit function;
 - (f) The organization of the function within a group or holding company;
 - (g) The professional competence, experience and expertise within the internal audit function;
 - (h) The remuneration structure of the head of the internal audit function and the key internal auditors; and
 - (i) Outsourced internal audit activities, if any.
- 17.3 The audit committee must develop and maintain its own tools to assess the quality of the internal audit function. The AMBD will conduct its own assessment of the quality of the internal audit function. Weaknesses identified in the internal audit function may affect the supervisor's assessment of the bank's risk profile.

- 17.4 The appointment and replacement of the head of the internal audit function is relevant to the AMBD's assessment of a bank. Therefore, the audit committee or senior management must promptly inform the AMBD of the appointment of a new head of the internal audit function, including relevant qualifications and previous experience. Similarly, whenever the head of the internal audit function ceases to act in this capacity, the AMBD must be informed of this fact and its circumstances. The AMBD will normally meet with the head of internal audit to discuss the reasons for his or her departure.

C. EARLY REMEDIAL ACTION BY AMBD

Principle:

18. The AMBD will formally report all weaknesses it identifies in the internal audit function to the board of directors and require remedial actions. The AMBD will take informal or formal supervisory actions requiring the board and senior management to remedy any identified deficiencies related to the internal audit function within a specified timeframe and to provide periodic written progress reports.

Guidelines:

- 18.1 If the AMBD concludes that a bank's internal audit function is inadequate or ineffective, it will require the board of directors to develop an appropriate written remediation plan that addresses the identified weaknesses on a timely basis. The written plan must be submitted to the AMBD for review. If the AMBD is not satisfied, it will require changes or additional measures to be included in the plan. The AMBD will monitor the implementation of the plan.
- 18.2 In addition to measures relating to the performance and standing of the internal audit function, the AMBD may also recommend enhancements to the governance of the bank including the functioning of the audit committee. Supervisory action may be of a public or non-public nature.
- 18.3 The audit committee and board of directors must not conclude that the internal audit function is functioning well solely because the AMBD has not identified any weaknesses. The supervisory review process is not a substitute for the audit committee's assessment, or an external assessment of the internal audit function.

Principle:

19. The AMBD will consider the impact of its assessment of the internal audit function on its evaluation of the bank's risk profile and on its own supervisory work.

Guidelines:

- 19.1 The assessment of the internal audit function will have consequences for the AMBD's evaluation of the bank's risk profile, the allocation of supervisory resources and the activities envisaged by the authority.
- 19.2 Where remedial actions cannot be agreed upon or where the bank faces ongoing delays in remediating the identified weaknesses, the AMBD will consider the impact of this on the bank's risk profile.
- 19.3 In cases where a bank belongs to an international group, the AMBD will consider sharing its concerns with the other relevant authorities, for example within the supervisory college.

Principle:

20. The supervisory authority will take informal or formal supervisory actions requiring the board and senior management to remedy any identified deficiencies related to the internal audit function within a specified time.

Guidelines:

- 20.1 While the AMBD expects banks to have a strong and robust internal audit function, there will be certain circumstances in which deficiencies exist and warrant specific supervisory actions aimed at remedying the deficiencies. Supervisory action may be of a public or non-public nature.

V. RESPONSIBILITIES OF A BANK'S AUDIT COMMITTEE

The audit committee prepares the work of, and reports to the board of directors in specific areas for which it has designated responsibility. The board of directors assumes final responsibility. The audit committee may invite the head of internal audit, the head of compliance, senior management, in particular the chief executive officer and other officials deemed relevant for the purpose of fulfilling its responsibilities to attend meetings of the committee. It is a sound practice that the head of internal audit and members of the audit committee have a private session, i.e. in the absence of management, to discuss issues of interest.

The main areas of responsibility of the audit committee are listed below by broad categories. (This listing does not detract from **the responsibilities summarized in the Guidelines of Corporate Governance for Banks.**) The list provides a summary of sound practices for the audit committee of a bank. This list may vary according to the structure of a bank and its practices.

Financial reporting, including disclosures

- (a) monitoring the financial reporting process and its output;
- (b) overseeing the establishment of accounting policies and practices by the bank and reviewing the significant qualitative aspects of the bank's accounting practices, including accounting estimates and financial statement disclosures;
- (c) monitoring the integrity of the bank's financial statements and any formal announcements relating to the bank's financial performance;
- (d) reviewing significant financial reporting judgments contained in the financial statements, including qualitative aspects of accounting practices such as estimates; and
- (e) reviewing arrangements by which staff of the bank may confidentially raise concerns about possible improprieties in matters of financial reporting.

Internal control

- (f) ensuring that senior management establishes and maintains an adequate and effective internal control system and processes. The system and processes must be designed to provide assurance in areas including reporting (financial, operational, risk), monitoring compliance with laws, regulations and internal policies, efficiency and effectiveness of operations and safeguarding of assets.

Audit

- (g) monitoring and reviewing the effectiveness of the bank's internal audit function;
- (h) approving the internal audit plan, scope and budget;
- (i) reviewing and discussing internal audit reports;
- (j) ensuring that the internal audit function maintains open communication with senior management, external auditors, the supervisory authority, and the audit committee;
- (k) reviewing discoveries of fraud and violations of laws and regulations as raised by the head of the internal audit function;
- (l) approving the audit charter and the code of ethics of the internal audit function;
- (m) approving, or recommending to the board for its approval, the annual remuneration of the internal audit function as a whole, including performance awards;
- (n) assessing the performance of the head of the internal audit function; and,
- (o) approving, or recommending to the board for its approval, the appointment, re-appointment or removal of the head of the internal audit function and the key internal auditors.

The statutory audit or external audit

Appointment, reappointment, dismissal and remuneration

- (p) approving a set of appropriate objective criteria for approving the statutory auditor or external audit firm of the bank;
- (q) Approving or recommending to the board or shareholders for their approval, the appointment, re-appointment and removal of the statutory auditor or external audit firm;
- (r) Approving the remuneration and terms of engagement of the statutory auditor or external audit firm.

Compliance with relevant ethical requirements, in particular independence and objectivity

- (s) reviewing and monitoring the independence of the statutory auditor or external audit firm, and in particular the provision of additional services to the bank, including the related safeguards that have been applied to eliminate identified threats to independence or reduce them to an acceptable level;
- (t) reviewing and monitoring the statutory auditor's objectivity and the effectiveness of the audit process;

- (u) developing and implementing a policy on the engagement of the statutory auditor or external audit firm for the supply of non-audit services, taking into account relevant ethical guidelines on the provision of non-audit services by the external audit firm; and
- (v) approving the total fees charged for the audit of the financial statements and for non-audit services provided by the external audit firm and external audit network firms to the bank and its group.

The statutory audit or external audit

- (w) overseeing the statutory audit of the annual and consolidated accounts;
- (x) discussing with the external auditor firm key matters arising from the statutory audit or external audit, and in particular any identified material weaknesses in internal control in relation to the financial reporting process; and
- (y) discussing the written representations the statutory auditor or external audit firm is requesting from senior management and, where appropriate, those charged with governance;

Remedial actions

- (z) ensuring that senior management is taking necessary corrective actions to address the findings and recommendations of internal auditors and external auditors in a timely manner;
- (aa) addressing control weaknesses, non-compliance with policies, laws and regulations and other problems identified by internal auditors and external auditors, and
- (bb) ensuring that deficiencies identified by AMBD related to the internal audit function are remedied within an appropriate time frame and that progress of necessary corrective actions are reported to the board of directors.

- E N D -